II. CLAIM AMENDMENTS

1-11 (Cancelled)

12. (New) A postal security device in the form of an application specific integrated circuit for providing cryptographic resources for a postal franking system comprising:

a cryptographic processor having a random number generator for generating cryptographic keys and executable cryptographic algorithms;

a non-volatile memory for securely storing said cryptographic keys;

a postal indicia processor for generating postal indicia in combination with cryptographic keys;

a communications bus for communicating with a host computer to initiate generation of postal indicia and allow a user of said postal security device to verify the authenticity of the postal indicia generated by said postal indicia processor by analyzing said cryptographic keys;

a physical security mechanism enclosing said application specific integrated circuit to prevent unauthorized access or modification of the cryptographic keys;

a clock circuit for secure time keeping of operations of the postal security device;

a time-out circuit for setting a time period for completing a transaction with said host computer and for terminating said transaction when said time period is exceeded; and

a non-accessible self test processor to perform analysis for the purpose of verifying full functionality of the postal security device.

13. (New) A postal security device, as described in claim 12, wherein said application specific integrated circuit is embodied in a PCMCIA card.

14. (New) A postal security device, as described in claim 12, wherein said non-volatile memory is not accessible and a further accessible memory is provided to store accounting, identification, and operational history data for a user.

15. (New) A postal security device, as described in claim 12, wherein said cryptographic algorithms generate a check sum representation of generated data to provide a unique digital signature which may be verified by a user.

16. (New) A postal security device, as described in claim 12, further comprising means for cooperative operation with a secure memory management unit in said host computer to isolate the cryptographic processor and prevent tampering with the generation of cryptographic keys.